UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/697,354	10/29/2003	Brian Harold Kelley	030622	7523

23696 7590 10/12/2007
QUALCOMM INCORPORATED
5775 MOREHOUSE DR.
SAN DIEGO, CA 92121

EXAMINER	
SHERKAT, AREZOO	
ART UNIT	PAPER NUMBER
2131	
NOTIFICATION DATE	DELIVERY MODE
10/12/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

us-docketing@qualcomm.com
kascanla@qualcomm.com
nanm@qualcomm.com

D

Office Action Summary	**Application No.** 10/697,354	**Applicant(s)** KELLEY ET AL.	
	Examiner Arezoo Sherkat	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 September 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19 and 24-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19 and 24-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Response to Amendment

This office action is responsive to Applicant's amendment received on 9/19/2007. Claims 1, 10, and 15 are amended. Claims 20-23 are cancelled. Claims 1-19, and 24-26 remain pending.

Response to Arguments

Applicant's arguments with respect to claims 1-19, and 24-26 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-19, and 24-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ellison et al., (U.S. Patent No. 6, 795,905 and Ellison hereinafter), in view of Christie et al., (U.S. Patent No. 7,130,951 and Christie hereinafter).

Regarding claims 1, 10, and 15, Ellison discloses a method wherein the operating modes comprise a privileged mode (i.e., isolated execution mode) and a non-privileged mode (i.e., normal execution mode)(col. 4, lines 13-25), and the method comprising:

enabling both the privileged (i.e., isolated) and the non-privileged (i.e., normal) modes if it is determined that the device is to operate in both the privileged and the non-privileged modes (col. 2, lines 47-50 and col. 3, lines 6-9)(i.e., Access to an accessible physical memory 60 is governed according to their ring hierarchy and the execution mode. ... the isolated area is accessible only to elements of the operating system and processor operating in an isolated execution mode. The non-isolated area 80 is accessible to all elements of the ring 0 operating system and to the processor), wherein programs operating in the privileged mode have unlimited access to device memory and/or device functions (i.e., the isolated execution ring-0 15, including the operating system nub 16 and the processor nub 18, can access both of the isolated area 70, including applet pages 72 and the nub pages 74, and the non-isolated area 80, including the application pages 82 and the operating system pages 84) and programs operating in the non-privileged mode have limited access to device memory and/or device functions (i.e., the normal execution ring-0 11, including the primary operating system 12 and software drivers 13, and hardware drivers 14, can access both of the non-isolated area 80, including the application pages 82 and the operating system pages 84, but cannot access the isolated area 70)(col. 4, lines 10-45 and col. 12, lines 5-41).

Ellison does not expressly disclose enabling the privileged mode during a device initialization if it is determined that the device is to operate only in the privileged mode.

However, Christie discloses a method for selectively enabling operating modes of a device during a device initialization, wherein the operating modes comprise a privileged mode (i.e., trusted execution mode, by the secure kernel) and a non-privileged mode (i.e., normal mode)(col. 12, lines 63-67 and col. 13, lines 1-30), and the method comprising:

determining during the device initialization whether the device is to operate in the privileged mode or in both the privileged and non-privileged modes, enabling the privileged mode if it is determined that the device is to operate only in the privileged mode (col. 12, lines 63-67 and col. 13, lines 1-30), and enabling the privileged mode if it is determined that the device is to operate only in the privileged mode (col. 8, lines 63-67 and col. 9, lines 1-67 and col. 13, lines 15-67 and col. 14, lines 1-62).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Ellison with teachings of Christie because it would allow to include a SEM processor as disclosed by Christie. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Christie to disable the plurality of interrupts from interrupting the secure execution mod-capable processor when it is operating in a secure execution mode (Christie, col. 3, lines 1-12).

Regarding claims 6 and 24, Ellison discloses two operating modes comprising a privileged mode (i.e., isolated execution mode) and a non-privileged mode (i.e., normal execution mode)(col. 4, lines 13-25), further comprising:

enabling both the privileged (i.e., isolated) and the non-privileged (i.e., normal) modes if it is determined that the device is to operate in both the privileged and the non-privileged modes (col. 2, lines 47-50 and col. 3, lines 6-9)(i.e., Access to an accessible physical memory 60 is governed according to their ring hierarchy and the execution mode. ... the isolated area is accessible only to elements of the operating system and processor operating in an isolated execution mode. The non-isolated area 80 is accessible to all elements of the ring 0 operating system and to the processor), wherein programs operating in the privileged mode have unlimited access to device memory and/or device functions (i.e., the isolated execution ring-0 15, including the operating system nub 16 and the processor nub 18, can access both of the isolated area 70, including applet pages 72 and the nub pages 74, and the non-isolated area 80, including the application pages 82 and the operating system pages 84) and programs operating in the non-privileged mode have limited access to device memory and/or device functions (i.e., the normal execution ring-0 11; including the primary operating system 12 and software drivers 13, and hardware drivers 14, can access both of the non-isolated area 80, including the application pages 82 and the operating system pages 84, but cannot access the isolated area 70)(col. 4, lines 10-45 and col. 12, lines 5-41).

Ellison does not expressly disclose enabling the privileged mode during a device initialization if it is determined that the device is to operate only in the privileged mode.

However, Christie further discloses a method for selectively enabling operating modes of a device during a device initialization, wherein the operating modes comprise a privileged mode (i.e., trusted execution mode, by the secure kernel) and a non-privileged mode (i.e., normal mode)(col. 12, lines 63-67 and col. 13, lines 1-30), a flag (i.e., SEM enable flag), and selection logic that operates to read the flag to set the operating mode of the device, wherein if the flag is set the selection logic enables the privileged mode, and if the flag is not set, the selection logic enables both the privileged and non-privileged modes (col. 11, lines 60-67 and col. 12, lines 1-20).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Ellison with teachings of Christie because it would allow to include a SEM processor as disclosed by Christie. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Christie to disable the plurality of interrupts from interrupting the secure execution mod-capable processor when it is operating in a secure execution mode (Christie, col. 3, lines 1-12).

As per claims 2, 11, and 16, Christie discloses wherein the step of determining comprises testing a flag (i.e., SEM enable flag)(col. 11, lines 60-67 and col. 12, lines 1-20).

As per claims 3, 12, and 17, Christie discloses wherein the step of enabling only the privileged mode comprises controlling one or more device memory management units to enable only the privileged mode (col. 7, lines 1-32).

As per claims 4, 13, and 18, Ellison discloses wherein the step of enabling both the privileged mode and the non-privileged modes comprises controlling one or more device memory management units to enable both modes (col. 2, lines 64-67 and col. 3, lines 1-67, and col. 4, lines 1-10, where it is inherent that the processor contains a MMU to manage communications with memory).

As per claims 5, 14, 9, and 19, Ellison discloses the method of claim 1, wherein the device is a wireless device (col. 2, lines 47-67 and col. 3, lines 1-67, and col. 4, lines 1-10, where the logical operating architecture may be realized to be deployed on a laptop).

As per claim 7, Christie discloses further comprising a memory that stores the flag (col. 11, lines 60-67 and col. 12, lines 1-20).

As per claim 8, Christie discloses further comprising one or more memory management units (i.e., memory controllers) that are controlled by the selection logic (i.e., MC control logic) to set the operating mode of the device (col. 9, lines 54-67 and col. 10, lines 1-67 and col. 11, lines 1-12).

Regarding claim 25, Ellison further discloses wherein the memory further comprises a code memory and a data memory, further comprising:

wherein the code memory is operable to store code (i.e., NUB pages 74 and OS pages 84)(col. 4, lines 10-50), a first memory management unit operable, under control of the selection logic, to partition (i.e., isolate) the code memory into a privileged code region comprising privileged code and a non-privileged code region comprising non-privileged code (col. 8, lines 20-67 and col. 9, lines 1-67), wherein the data memory is operable to store data (i.e., Applet pages 72 and Application pages 82)(col. 4, lines 10-50), and a second memory management unit operable, under control of the selection logic, to partition the data memory into a privileged data region comprising privileged data and a non-privileged data region comprising non-privileged data (col. 8, lines 20-67 and col. 9, lines 1-67).

Regarding claim 26, Ellison further discloses wherein the first memory management unit is operable to restrict operation of the non-privileged code to the non-privileged code region of the code memory, and wherein the second memory management unit is operable to restrict operation of the non-privileged code to the non-privileged data region of the data memory (i.e., Access to an accessible physical memory 60 is governed according to their ring hierarchy and the execution mode. ... the isolated area is accessible only to elements of the operating system and processor operating in an isolated execution mode. The non-isolated area 80 is accessible to all elements of the ring 0 operating system and to the processor)(col. 4, lines 10-45).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Arezoo Sherkat whose telephone number is (571) 272-3796. The examiner can normally be reached on 8:00-4:30 Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

A.S.
Patent Examiner
Group 2131
October 3, 2007

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100